REMARKS

Favorable reconsideration and allowance of the claims of the present application are respectfully submitted.

Claims 1-21 are rejected. Particularly, Claims 1-4, 12-14, 21 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Brennan et al. (U.S. Patent No. 5,675,649) (hereafter "Brennan") in view of Arditti et al. (U.S. Patent No. 6,125,445) (hereafter "Arditti"). Moreover, Claims 5, 15-16 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Brennan in view of Boudot (Eurocrypt 200, LNCS 1807, pp. 431-444, 200) (hereafter "Boudot"). Furthermore, Claim 6 stands rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Brennan in view of Boudot as applied to Claim 5 above, and in further view of Matyas et al. (U.S. Patent No. 5,265,164) (hereafter "Matyas"). In addition, Claims 7-8, 10, 17-18, 20 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Chaum (U.S. Patent No. 4,996,711) (hereafter "Chaum") in view of Boudot. Moreover, Claims 9, 11, 19 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Hopkins et al. (U.S. Patent Application No. 2003/0120931) (hereafter "Hopkins") in view of Boudot. Furthermore, Claims 11, 13-21 stand objected to under 37 C.F.R. 1.75(c), as being improper dependent form as allegedly failing to further limit the subject matter of a previous claim.

Applicants provide the following response to the objection and respectfully traverse rejections presented in the May 16, 2007 Office Action.

In reviewing the status of the claims, Applicants have amended independent Claims 1, 5, 7, 9, 10 and 12, for aesthetic reasons to remove the dashes preceding each element of those claims.

With regards to the objection to Claims 11, 13-21, Claims 14, 16 and 18 have been amended in proper *Beauregard* form, to recite a computer program storage device, readable by machine, tangibly embodying a program of instructions executable by a machine. In re Beauregard, 53 F.3d 1583 (Fed. Cir. 1995). Dependent Claims 11, 13, 15, 17 and 19-21 have been canceled thereby rendering the object to those claims moot.

In canceling dependent Claims 11, 13, 15, 17 and 19-21, Applicants are not conceding in this application that those claims are not patentable, as the present claim amendments and cancellations are only for facilitating expeditious prosecution of the claims in this case. Applicants respectfully reserve the right to pursue these and other claims in one or more continuations and/or divisional patent applications.

Therefore, Applicants respectfully request withdrawal of this ground of objection.

With regards to obviousness rejections of Claims 1 - 4, 12-14, 21 as allegedly being unpatentable over Brennan in view of Arditti, and the obviousness rejections of Claims 5, 15-16 as allegedly being unpatentable over Brennan in view of Boudot.

Claim 1, as amended, recites a method for providing cryptographic keys usable in a network of connected computer nodes applying a signature scheme, the method executable by a first computer node comprising the steps of, *inter alia*, **generating an exponent interval having a first random limit** . . . **each element of the exponent interval has a unique prime factor** . . . and providing **a public key** *comprising an exponent-interval description* and a public key value derived from the random secret key, **such that the random secret key and a selected exponent**

value from the exponent interval are usable for deriving a signature value on a message to be sent within the network to a second computer node for verification. Similarly, Claim 5 recites similar features.

In contrast, Brennan discloses a cryptographic key generation and safekeeping process whereby source code is loaded on a secure computer system with a "master-key" and "locking-key" complied from the source code and then stored on disks (Abstract, Col. 12, lines 43-46). Moreover, Brennan describes a "public exponent e" which is derived from an RSA modulus N and private exponent d. (Col. 9, lines 19-28). In addition, Brennan asserts that "[t]he random number generator built in this stage produces random integers **uniformly between two selected bounds**, in a way that is provably hard to predict." (Col. 10, lines 39-41) (Emphasis added). And "p, and q all have approximately the same number of bits in their binary expansion. Lastly, the factors p and q are chosen so that (p-1)/2 and (q-1)/2 are odd integers, and x must not be divisible by p or q." Nowhere in Brennan's disclosure does it mention that **each element** of the **exponent interval has a unique prime factor** as recited in both independent Claims 1 and 5. In other words, random integers **uniformly between two selected bounds** produced in Brennan can have multiple occurrences where the prime factors are the same – hence not unique prime factors. Therefore Brennan fails to suggest or teach **generating an exponent interval having a first random limit** . . . **each element of the exponent interval has a unique prime factor** as recited in the Claims 1 and 5. Similarly, Arditti, also fails to suggest or teach the methods of Claims 1 and 5 where **each element of the exponent interval has a unique prime factor.**

Applicants also note that the Office Action fails to appreciate that the present invention, as recited in Claims 1 and 5, generates a **public key value** derived from the random secret key, **such that the random secret key and a selected exponent value from the exponent interval**

are usable for deriving a signature value on a message to be sent within the network to a second computer node for verification. The public keys of Brennan and Arditti, as discussed above, do not generate public keys as claimed in the present invention for at least the reason that those prior art references fail to generate a public key having **an exponent interval having a first random limit** . . . **each element of the exponent interval has a unique prime factor** as recited in Claims 1 and 5.

Moreover, as mentioned above, in the case of Brennan, no signature value on a message is derived by the **first computer node**, instead Brennan provides for a "master-key" and "locking-key" which are compiled from Brennan's source code on *shared* disks on *several* computers (Col. 12, lines 43-46). In other words, Brennan fails to generate a **public key value** derived from the random secret key, **such that the random secret key and a selected exponent value from the exponent interval are usable for deriving a signature value on a message to be sent within the network to a second computer node for verification** as disclosed in Claims 1 and 5. In the case of Arditti, a "claimant" draws a first random number α and calculates a value while a "verifier" draws a second random exponent β and calculates a value (abstract). Arditti defines the claimant and verifier as two different entities (Col. 1, lines 21-23). In other words, Arditti fails to suggest or teach generate a **public key value** derived from the random secret key, **such that the random secret key and a selected exponent value from the exponent interval are usable for deriving a signature value on a message to be sent within the network to a second computer node for verification** as recited in the Claims 1 and 5.

Therefore, since both Brennan and Arditti fail to suggest or teach at least two features set forth in Claims 1 and 5, they both fail to make obvious the present invention as recited in those claims. Applicants respectfully request withdrawal of this rejection.

With regards to the obviousness rejections of Claims 7-8, 10, 17-18, 20 as allegedly being unpatentable over Chaum in view of Boudot.

Claim 7, as amended, recites a method for verifying a signature value on a message in a network of connected computer nodes, the method executable by a **second computer node** comprising the steps of, *inter alia* verifying whether an exponent value is contained in an exponent interval, wherein **each element of the exponent interval** has, with a probability close to certainty, **a unique prime factor** that is **larger than a given security parameter**, the signature value is invalid if the exponent value is not contained in the exponent interval. Similarly, Claim 10, as amended recites similar features.

In contrast, Chaum discloses that "at least one prime factor" is uniquely determined by the message. In other words, Chaum fails to suggest or teach **each element of the exponent interval** having **a unique prime factor** that is **larger than a given security parameter**. Only one of Chaum's prime factors has to be unique, it does not mention its relationship with any security parameter and the prime factors in Chaum's are relevant to the message not an interval.

Boudot fails to remedy Chaum's deficiency and merely provides a rather abstract proof related to "membership to an interval" where there is no mention of **each element of the exponent interval** having **a unique prime factor** that is **larger than a given security parameter** as recited in Claim 7 and 10.

Therefore, since both Chaum and Boudot fail to suggest or teach at least two features set forth in Claim 7, they both fail to make obvious the present invention as recited in those claims. Since dependent Claim 8 depends from allowable Claim 7, it is also considered allowable. Claims 17 and 20, as mentioned above, have been canceled and therefore the rejection of those claims is now moot. Claim 18, as mentioned above is now in proper *Beauregard* form and

contain similar features as Claims 7 and 10, therefore Applicants believe that it is similarly allowable. Applicants respectfully request withdrawal of this rejection.

With regards to the obviousness rejections of Claims 9, 11, 19 which stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Hopkins in view of Boudot.

Claim 9, as amended, recites an apparatus to provide a signature value on a message in a network of connected computer nodes, the apparatus executable by a first computer node comprising, *inter alia*, means for selecting an exponent value from an exponent interval, wherein **each element of the exponent interval has**, with a probability close to certainty, **a unique prime factor that is larger than a given security parameter**. Claim 11 as amended recites similar features.

In contrast, Hopkins recites a method of generating a group of digital signatures where an associated individual modulus is formed by, *inter alia* "one or more k prime factors of the group." No where in Hopkins disclosure does it mention that **each element of the exponent interval has . . . a unique prime factor that is larger than a given security parameter** as recited in Claim 9.

As discussed in response to the rejection to Claims 7-8, 10, 17-18, 20, Boudot similarly fails to remedy Hopkins' deficiency and merely provides a rather abstract proof related to "membership to an interval" where there is no mention of **each element of the exponent interval** having **a unique prime factor** that is **larger than a given security parameter** as recited in Claim 9.

Therefore, since both Hopkins and Boudot fail to suggest or teach at least two features set forth in Claim 9, they both fail to make obvious the present invention as recited in those claims. Applicants respectfully request withdrawal of this rejection.

With regards to the obviousness rejection of dependent Claim 6, which stands rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Brennan in view of Boudot as applied to Claim 5 above, and in further view of Matyas. Applicants note that since it is believed that independent Claim 5 is allowable that dependent Claim 6, which depends therefrom, is also allowable.

Therefore, Applicants respectfully request withdrawal of this rejection.

Thus, in view of the foregoing amendments and remarks, it is firmly believed that the present case is in condition for allowance, which action is earnestly solicited.

Respectfully Submitted,

Steven Fischman
Registration No. 34,594

Scully, Scott, Murphy & Presser, P.C.
400 Garden City Plaza – Suite 300
Garden City, New York 11530
(516) 742-4343
SF:DJD:tam